

	<div>Montana Operations Manual</div> <div><i>Policy</i></div>	Policy Number	1240.X13
		Effective Date	October 1, 2004
		Last Revised	June 30, 2011
Issuing Authority	State of Montana Chief Information Officer		
Workstation, Portable computer and PDA (Personal Digital Assistant) Security			

## I. Purpose

This Workstation, Portable Computer, and PDA (Personal Digital Assistant) Security Policy (Policy) is intended to establish minimum standards for the security of workstations, portable computers and PDA's owned by the State of Montana.

## II. Scope

This Policy encompasses information and information systems for which agencies have administrative responsibility, including information and systems managed or hosted by third-parties on agencies' behalf.

This Policy may conflict with other information system policies currently in effect. Where conflicts exist, the more restrictive policy governs. The development of future policies or standards will specifically identify and retire any superseded portions of current policies or standards.

## III. Authority

Pursuant to the Montana Information Technology Act (MITA) (Title 2, Chapter 17, Part 5 of the Montana Code Annotated (MCA)), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. [§2-17-505\(1\) MCA](#).

It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. [§2-17-505\(2\) MCA](#).

## **IV. Roles And Responsibilities**

### **A. Department of Administration**

Under MITA, the Department of Administration (DOA) is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. [§2-17-512 MCA](#).

### **B. Department Heads**

Each department head is responsible for ensuring an adequate level of security for all data within their department. [§2-15-114 MCA](#).

## **V. Applicability**

This Policy is applicable to agencies, staff and all others, including outsourced third-parties (such as contractors, or other service providers), who have access to, or use or manage information assets subject to the policy and standard provisions of [§2-17-534 MCA](#). This Policy shall be communicated to staff and others who have access to or manage information, and information systems and assets.

This policy applies to personal computers, other computing devices, and accessory equipment that store electronic data, information, and software programs.

## **VI. Definitions**

**Portable** A portable computer includes a laptop, pocket PC, tablet, or notebook, portable computers (such as Personal Digital Assistants [PDAs], smart phones, etc.), and any other computers being used to connect to the state's network remotely.

## **VII. Requirements**

Computer users are responsible for maintaining the physical security of their own workstation, portable computer, and/or PDA and for following the security requirements implemented by the Department of Administration and by the agency at which they are employed. Workstations, portable computers, and PDA's should be kept out of sight and covered when stored in a vehicle.

Any software installed on workstations, portable computers or PDA's that uses script files must not contain a userID or password for the state's computer system.

Workstations with unattended processes running on them must have some type of screen saver with password protection or keyboard locking program enabled on them.

Portable computers MUST be transported as carry-on luggage when traveling by plane or bus, unless the carrier requires otherwise.

All workstations, portable computers, and PDA's must be updated with the latest security patches, virus scanning software and virus data files. Agencies are responsible for installing the patches, virus scanning software and virus data files on their devices. Patches and updates to virus data files should be installed through an automated process if applicable. Agencies are required to install patches for high-risk vulnerabilities within 48 hours of notification.

Firewall software must be installed, updated, and used according to standards set by ITSD on all portable computers used to connect outside of the state (Internet) firewall.

All PDA's used to connect directly to state computers must be state owned. Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form.

## **VIII. Background - History On The Creation Of Or Changes To This Policy**

This policy was originally created by the NetWare Managers Group Policy Committee. This policy was updated by the Security Section of ITSD in January 2002 and reviewed with the Information Technology Managers Council prior to adoption.

## **IX. Guidelines - Recommendations, Not Requirements**

If highly sensitive or confidential information is stored on a portable computer or PDA, the data should be encrypted.

In accordance with ENT-SEC-071, the following information should appear on portable computers when powered on: "This computer is the property of the State of Montana, Department of <department name> and subject to the appropriate use policies located at: <http://itsd.mt.gov/policy/itpolicy.asp>. Unauthorized use is a violation of 45-6-311, MCA."

Power on or system passwords should be used on workstations that are in highly accessible areas and on portable computers. Power on passwords should be provided to the Network Administrator and kept in a secure place.

Patches and updates should be completed with an automated process if applicable.

## **X. Change Control and Exceptions**

Policy changes or exceptions are governed by the [Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards](#). Requests for a review or change to this instrument are made by submitting an Action Request form (at <http://sitsd.mt.gov/policy/policies/default.mcpX>). Requests for exceptions are made by submitting an Exception Request form (at <http://sitsd.mt.gov/policy/policies/default.mcpX>). Changes to policies and standards will be prioritized and acted upon based on impact and need.

## **XI. Closing**

Direct questions or comments about this instrument to the State of Montana Chief Information Officer at ITSD Service Desk (at <http://servicedesk.mt.gov/ess.do>), or:

PO Box 200113  
Helena, MT 59620-0113  
(406) 444-2700  
FAX: (406) 444-2701

## **XII. References**

### **A. Legislation**

1. [§2-17-505\(1\) MCA](#) – Policy
2. [§2-17-514\(1\) MCA](#) – Enforcement
3. [§2-17-505\(2\) MCA](#)
4. [§2-17-512 MCA](#)
5. [§2-15-114 MCA](#)
6. [§2-15-112 MCA](#)

### **B. Policies, Directives, Regulations, Rules, Procedures, Memoranda**

1. House Joint Resolution No. 31
2. MOM 3-0130 Discipline
3. MOM 1-0250
4. MOM 3-0620 (now included in MOM 3-0630 )

5. ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
6. ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.
7. Statewide Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
8. Statewide Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

### **XIII. Administrative Use**

**A. Scheduled Review Date:** April 13, 2014

**B. Changes:** July 11, 2008 – Non-material changes made:

- Standardize instrument format and common components
- Changed to reflect next review date

April 7, 2009 – Non-material changes made:

- Corrected broken URLs
- Applied new document layout.

May 4, 2009 – Non-material changes made:

- Deleted Incorrect version number field number

June 8, 2010 – Non-material changes made:

- Corrected URLs.

June 30, 2011 – Non-material changes made:

- Corrected broken URLs
- Changed to MoM Format